

# CONSTRUCTIONS OF STRONGLY REGULAR CAYLEY GRAPHS USING EVEN INDEX GAUSS SUMS

FAN WU

**ABSTRACT.** In this paper, generalizing the result in [11], we construct strongly regular Cayley graphs by using union of cyclotomic classes of  $\mathbb{F}_q$  and Gauss sums of index  $w$ , where  $w \geq 2$  is even. In particular, we obtain three infinite families of strongly regular graphs with new parameters.

## 1. INTRODUCTION

We assume that the reader is familiar with the basic theory of strongly regular graphs as can found in [4, 12, 20]. All graphs considered in this paper are simple and undirected.

A *strongly regular graph*  $\text{srg}(v, k, \lambda, \mu)$  is a regular graph of order  $v$  and valency  $k$ , neither complete nor edgeless, which has the following properties:

- (1) Any two adjacent vertices have exactly  $\lambda$  common neighbors.
- (2) Any two nonadjacent vertices have exactly  $\mu$  common neighbors.

Strongly regular graphs have been studied extensively since their introduction by Bose [2] in 1963. In this paper, we will only be concerned with strongly regular Cayley graphs, which are  $\text{srg}$  with an automorphism group acting sharply transitively on the vertex sets. Such  $\text{srg}$  are closely related to two-weight linear codes, projective two-intersection sets in finite geometry, and partial difference sets. We refer the reader to [16], [4], [19] for these connections.

Let  $\Gamma$  be a graph and  $A$  be its adjacency matrix. Then  $A$  is a symmetric  $(0, 1)$ -matrix with all its diagonal entries being zero. The *eigenvalues* of  $\Gamma$  are by definition the eigenvalues of  $A$ . Below is a spectral characterization of  $\text{srg}$ ; see [4, p. 115] for a proof. For convenience, we call an eigenvalue of  $\Gamma$  *restricted* if it has an eigenvector orthogonal to the all-one vector.

**Theorem 1.1.** *For a regular graph  $\Gamma$  of order  $v$  and valency  $k$ , not complete nor edgeless, with adjacency matrix  $A$ , the following are equivalent:*

- (1)  $\Gamma$  is an  $\text{srg}(v, k, \lambda, \mu)$  for certain integers  $\lambda, \mu$ .
- (2)  $A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$ , where  $I, J$  are the identity matrix and the all-ones matrix, respectively.
- (3)  $A$  has precisely two distinct restricted eigenvalues.

Let  $q$  be a prime power,  $\mathbb{F}_q$  be the finite field of order  $q$ , and  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ . Let  $D$  be a subset of  $\mathbb{F}_q^*$  such that  $-D = D$ . The *Cayley graph*  $\text{Cay}(\mathbb{F}_q, D)$  is the graph whose vertex set is  $\mathbb{F}_q$ , and two vertices are adjacent if and only if their difference belongs to  $D$ . Let  $D$  be a subgroup of  $\mathbb{F}_q^*$  such that  $-D = D$ . If  $\text{Cay}(\mathbb{F}_q, D)$  is an  $\text{srg}$ , then we say that  $\text{Cay}(\mathbb{F}_q, D)$  is a *cyclotomic strongly regular graph*. As an example of cyclotomic  $\text{srg}$ , we mention the Paley graph  $P(q)$ ,

which is nothing but  $\text{Cay}(\mathbb{F}_q, D)$ , where  $D$  is the subgroup of  $\mathbb{F}_q^*$  of index 2, and  $q$  is a prime power congruent to 1 modulo 4.

Cyclotomic strongly regular graphs have been extensively studied. Let  $p$  be a prime,  $f$  a positive integer, and  $D$  be a subgroup of  $\mathbb{F}_{p^f}^*$  of index  $N > 1$ . If  $D$  is the multiplicative group of a subfield of  $\mathbb{F}_{p^f}$ , then it is easy to see that  $\text{Cay}(\mathbb{F}_{p^f}, D)$  is an srg. Such cyclotomic srg are called *subfield examples*. Next, if there exists a positive integer  $t$  such that  $-1 \equiv p^t \pmod{N}$ , then it can be shown that  $\text{Cay}(\mathbb{F}_q, D)$  is an srg. (For a proof of this fact, see [5].) Such cyclotomic srg are called *semi-primitive examples*. Schmidt and White [19] proposed a conjectural classification of all cyclotomic srg. We state their conjecture below.

**Conjecture 1.2.** (Conjecture 4.4, [19]) *Let  $p$  be a prime,  $f$  a positive integer, and  $q = p^f$ . Let  $N > 1$  be a divisor of  $(q - 1)/(p - 1)$ . Assume that  $D$  is the subgroup of  $\mathbb{F}_q^*$  of index  $N$  such that  $-D = D$ . If  $\text{Cay}(\mathbb{F}_q, D)$  is an srg, then one of the following holds:*

- (1) (*subfield case*)  $D = \mathbb{F}_{p^e}^*$  for some integer  $e \geq 1$ ,  $e|f$ .
- (2) (*semi-primitive case*) There exists a positive integer  $t$  such that  $-1 \equiv p^t \pmod{N}$ .
- (3) (*exceptional case*)  $\text{Cay}(\mathbb{F}_{p^f}, D)$  is one of the 11 sporadic examples appearing in the following table:

$N$	$p$	$f$	$[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle]$
11	3	5	2
19	5	9	2
35	3	12	2
37	7	9	4
43	11	7	6
67	17	33	2
107	3	53	2
133	5	18	6
163	41	81	2
323	3	144	2
499	5	249	2

Table I

Partial results on Conjecture 1.2 can be found in [19, 1]. However the conjecture as a whole remains open. On the other hand, in a series recent papers [9, 10, 11], by using unions of cyclotomic classes of  $\mathbb{F}_q$  (instead of using a single cyclotomic class), it is shown that most of the examples in Table I can be generalized into infinite families. Specifically, all index 2 examples but the first one, and the index 4 example in Table I have been generalized into infinite families. The constructions in [9, 10, 11] rely on explicit determination of index 2 or 4 Gauss sums. A natural question arises: can constructions similar to those in [9, 10, 11] produce srg in high index cases? In particular, can one generalize the index 6 examples in Table I into infinite families. A major obstacle is the determination of Gauss sums of high indices. After studying [11] closely, we realize that in order to construct strongly regular Cayley graphs by using methods similar to those in [9, 10, 11], one does not need to evaluate Gauss sums of high indices explicitly; it suffices to know which subfield (of the cyclotomic field) the Gauss sums belong to. The results of the paper are as follows. We first generalize the construction of [11] to the index  $w$  case, where  $w \geq 2$  is even. See Theorem 3.2. This step is straightforward.

The main new result is Theorem 3.3, in which we give necessary and sufficient conditions for the construction in Theorem 3.2 to give srg. In Section 4, we use these results to construct explicit families of srg. In particular, we obtain three infinite families of srg. The first family generalizes Example 5 in Table I. The second and third families of srg generalize some subfield examples of cyclotomic strongly regular graphs.

## 2. GAUSS SUMS

Let  $p$  be a prime,  $f$  be a positive integer, and  $q = p^f$ . Let  $\mathbb{F}_q$  be the finite field of order  $q$ . Let  $\xi_p$  be a fixed complex primitive  $p^{\text{th}}$  root of unity, and  $\text{Tr}_{q/p}$  be the trace from  $\mathbb{F}_q$  to  $\mathbb{F}_p$ . The *additive characters* of  $\mathbb{F}_q$  are the homomorphisms from the additive group  $(\mathbb{F}_q, +)$  to  $\mathbb{C}^*$ , the multiplicative group of  $\mathbb{C}$ , and they are given by

$$\psi_a(x) = \xi_p^{\text{Tr}_{q/p}(ax)},$$

where  $a \in \mathbb{F}_q$ . We usually write  $\psi_1$  simply as  $\psi$ , which is called the *canonical* additive character of  $\mathbb{F}_q$ . The *multiplicative characters* of  $\mathbb{F}_q$  are the homomorphisms from the multiplicative group  $\mathbb{F}_q^*$  to  $\mathbb{C}^*$ .

Let  $N$  be a positive integer with  $N \mid (q - 1)$ , and let  $\chi$  be a multiplicative character of  $\mathbb{F}_q$  of order  $N$ . The *Gauss sum*  $g(\chi)$  of order  $N$  is defined by

$$g(\chi) = \sum_{a \in \mathbb{F}_q^*} \chi(a) \psi(a).$$

Clearly Gauss sums of order  $N$  belong to  $\mathbb{Z}[\xi_N, \xi_p]$ , the integer ring of  $\mathbb{Q}(\xi_N, \xi_p)$ , where  $\xi_N$  is a primitive  $N^{\text{th}}$  root of unity. Let  $\sigma_{a,b}$  be the Galois automorphism of  $\mathbb{Q}(\xi_N, \xi_p)$  defined by

$$\sigma_{a,b}(\xi_N) = \xi_N^a, \quad \sigma_{a,b}(\xi_p) = \xi_p^b$$

The following lemma gives some useful properties of Gauss sums. For a proof of the lemma, we refer the reader to [3, p. 10] and [14, p. 208].

**Lemma 2.1.** *Let  $\chi$  be a multiplicative character of  $\mathbb{F}_q$  of order  $N$ . Then*

- (1)  $g(\chi) = -1$ , if  $\chi = \chi_0$  (the trivial character), and  $|g(\chi)| = q$ , if  $\chi \neq \chi_0$ .
- (2)  $\overline{\sigma_{a,b}(g(\chi))} = \overline{\chi^a(b)} g(\chi^a)$ , where  $\overline{\chi} = \chi^{-1}$ .
- (3)  $\overline{g(\chi)} = \chi(-1) g(\overline{\chi})$ , and  $\sigma_{p,1}(g(\chi)) = g(\chi^p) = g(\chi)$ .
- (4) For a character  $\chi$  of order  $N$ ,  $g(\chi)^N \in \mathbb{Z}[\xi_N]$ .

For the rest of this paper, we assume that (i)  $\gcd(p(p-1), N) = 1$ , where  $N \mid (q-1)$ , and  $q = p^f$ ,  $f$  is the order of  $p$  modulo  $N$ , (ii)  $-1 \notin \langle p \rangle$ , the cyclic subgroup of  $(\mathbb{Z}/N\mathbb{Z})^*$  generated by  $p$ . These assumptions have the following consequences.

First, the index  $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle]$ , denoted by  $w$ , must be even. This can be seen as follows. From  $\gcd(p(p-1), N) = 1$ , we see that  $N$  is odd. Thus  $\phi(N)$  is even, where  $\phi$  is the Euler totient function. If  $w$  is odd, then  $f = \phi(N)/w$  is even. It follows that  $p^{f/2} \equiv -1 \pmod{N}$ , contradicting the assumption that  $-1 \notin \langle p \rangle$ .

Secondly, let  $\chi$  be a multiplicative character of  $\mathbb{F}_q$  of order  $N$ . We claim that  $g(\chi) \in \mathbb{Z}[\xi_N]$ . We prove this claim as follows. For any  $b \in \mathbb{F}_p^*$ , since  $\gcd(N, p-1) = 1$ , we have  $\chi(b) = 1$ . Hence by Part (2) of Lemma 2.1,  $\sigma_{1,b}(g(\chi)) = \overline{\chi}(b) g(\chi) = g(\chi)$ . It follows that  $g(\chi) \in \mathbb{Z}[\xi_N]$ . We can actually go a little further. Let  $K$  be the decomposition field of the prime  $p$  in  $\mathbb{Q}(\xi_N)$ .

Then it is well known [14, p. 197] that  $\text{Gal}(\mathbb{Q}(\xi_N)/K) = \langle \sigma_{p,1} \rangle$ . By Part (3) of Lemma 2.1, we have  $g(\chi) \in K$ . In fact, we have  $g(\chi) \in O_K$ , the integer ring of  $K$ .

Gauss sums  $g(\chi)$  with  $\chi$  being a multiplicative character of order  $N$  of  $\mathbb{F}_q$  (and  $-1 \notin \langle p \rangle$ ) are called *Gauss sums of index  $w$* .

For the remainder of this paper we will further assume that  $N = p_1^m$ , where  $p_1$  is an odd prime,  $m \geq 1$  is an integer, and  $w|(p_1 - 1)$ . In this case,  $\text{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$  is cyclic, and  $K$  is the unique imaginary subfield of  $\mathbb{Q}(\xi_N)$  with  $[K : \mathbb{Q}] = w$ . Since  $w|(p_1 - 1)$ , we see that  $K$  is in fact a subfield of  $\mathbb{Q}(\xi_{p_1})$ . Therefore if  $\chi$  is a multiplicative character of  $\mathbb{F}_q$  of order  $N$ , we in fact have  $g(\chi) \in \mathbb{Z}[\xi_{p_1}]$ .

Let  $g$  be a primitive root modulo  $p_1$ . Define  $\widetilde{C}_j = g^j \langle p \rangle \subseteq (\mathbb{Z}/p_1\mathbb{Z})^*$ , for all  $0 \leq j \leq w - 1$ . Then  $(\mathbb{Z}/p_1\mathbb{Z})^* = \cup_{j=0}^{w-1} \widetilde{C}_j$ . For  $0 \leq j \leq w - 1$ , we define  $\eta_j$  by

$$\eta_j = \sum_{a \in \widetilde{C}_j} \xi_{p_1}^a, \quad (2.1)$$

where  $\xi_{p_1}$  is a complex primitive  $p_1$ -th root of unity. The following lemma is well known (see [18]).

**Lemma 2.2.** *With the above assumptions,  $\{\eta_j \mid 0 \leq j \leq w - 1\}$  is an integral basis of  $K$ .*

Let  $\chi$  be a multiplicative character of  $\mathbb{F}_q$  of order  $N$ . Let  $r$  be the largest nonnegative integer such that  $p^r | g(\chi)$ . That is,  $p^{-r}g(\chi) \in O_K$ , but  $p^{-(r+1)}g(\chi) \notin O_K$ . Note that if  $\chi'$  is another multiplicative character of  $\mathbb{F}_q$  of order  $N$ , then there exists a  $d \in (\mathbb{Z}/N\mathbb{Z})^*$  such that  $\chi' = \chi^d$ ; it follows that  $g(\chi') = g(\chi^d) = \sigma_{d,1}(g(\chi))$ . This shows that the integer  $r$  does not depend on the choice of the multiplicative character of order  $N$ . The explicit computation of  $r$  can be done by using Stickelberger's theorem on the prime ideal factorization of Gauss sums. We state the following lemma, whose proof can be found in [8].

**Lemma 2.3.** *Let  $\chi$  be a multiplicative character of  $\mathbb{F}_q$  of order  $N$ . With the above assumptions and notation, we have*

$$r = \frac{f - \tilde{f}}{2} + b,$$

where  $\tilde{f} = \frac{p_1 - 1}{w}$ ,  $b = \min\{b_0, b_1, \dots, b_{w-1}\}$  and  $b_j = \frac{1}{p_1} \sum_{z \in ([1, p_1 - 1] \cap \widetilde{C}_j)} z$  for all  $0 \leq j \leq w - 1$ , here  $[1, p_1 - 1]$  denotes the set of integers  $x$ ,  $1 \leq x \leq p_1 - 1$ .

### 3. CYCLOTOMIC CLASSES AND STRONGLY REGULAR CAYLEY GRAPHS

In this section,  $N$ ,  $p_1$ ,  $p$ ,  $f$  and  $w$  are the same as those in Section 2. Let  $\mathbb{F}_q$  be the finite field of order  $q$ ,  $q = p^f$ . Let  $\gamma$  be a fixed primitive element of  $\mathbb{F}_q$ . The  $N^{\text{th}}$  *cyclotomic classes*  $C_0, C_1, \dots, C_{N-1}$  of  $\mathbb{F}_q$  are defined by

$$C_i := \{\gamma^{i+jN} \mid 0 \leq j \leq \frac{q-1}{N} - 1\},$$

where  $0 \leq i \leq N - 1$ . Clearly  $C_i = \gamma^i C_0$ , for  $0 \leq i \leq N - 1$ . Let  $\psi$  be the canonical additive character of  $\mathbb{F}_q$ . The  $N^{\text{th}}$  *cyclotomic periods* (also known as *Gauss periods*) are defined by

$$\tau_a := \sum_{x \in C_a} \psi(x), \quad (3.1)$$

where  $0 \leq a \leq N - 1$ .

Let  $\widehat{\mathbb{F}_q^*}$  be the group of multiplicative characters of  $\mathbb{F}_q$ . Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of the additive characters in terms of the multiplicative characters of  $\mathbb{F}_q$ . That is,

$$\psi(a) = \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\overline{\chi}) \chi(a), \text{ for all } a \in \mathbb{F}_q^* \quad (3.2)$$

where  $\overline{\chi} = \chi^{-1}$ . Using (3.2), we obtain the relationship between Gauss sums and Gauss periods.

**Lemma 3.1.** *For  $0 \leq a \leq N - 1$ , we have*

$$\tau_a = \frac{1}{N} \sum_{\chi \in C_0^\perp} g(\overline{\chi}) \chi(\gamma^a), \quad (3.3)$$

where  $C_0^\perp$  is the subgroup of  $\widehat{\mathbb{F}_q^*}$  consisting of characters which are trivial on  $C_0$ .

**Proof:** From (3.1) and (3.2), we have

$$\begin{aligned} \tau_a &= \sum_{x \in C_0} \psi(\gamma^a x) = \frac{1}{q-1} \sum_{x \in C_0} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\overline{\chi}) \chi(\gamma^a x) \\ &= \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \sum_{x \in C_0} g(\overline{\chi}) \chi(\gamma^a x) \\ &= \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\overline{\chi}) \chi(\gamma^a) \sum_{x \in C_0} \chi(x) \end{aligned}$$

If  $\chi \notin C_0^\perp$ , then there exists a positive integer  $\ell$  such that  $\chi(\gamma^{\ell N}) \neq 1$ . We have

$$\chi(\gamma^{\ell N}) \sum_{x \in C_0} \chi(x) = \sum_{x \in C_0} \chi(\gamma^{\ell N} x) = \sum_{x \in C_0} \chi(x).$$

It follows that  $\sum_{x \in C_0} \chi(x) = 0$  since  $\chi(\gamma^{\ell N}) \neq 1$ . If  $\chi \in C_0^\perp$ , clearly  $\sum_{x \in C_0} \chi(x) = |C_0| = (q-1)/N$ . The proof of the lemma is now complete.  $\square$

Define

$$D := \bigcup_{i=0}^{p_1^{m-1}-1} C_i. \quad (3.4)$$

Using  $D$  as connection set, we construct  $\text{Cay}(\mathbb{F}_q, D)$ .

**Theorem 3.2.** *The Cayley graph  $\text{Cay}(\mathbb{F}_q, D)$  is an undirected regular graph of valency  $|D|$ . It has at most  $w + 1$  distinct restricted eigenvalues.*

The proof is parallel to that of Theorem 3.1 in [11]. Since we will use some parts of the proof later on, we will give the complete proof here.

**Proof:** Since  $N = p_1^m$  is odd, we have  $2N \mid (q-1)$  or  $q$  is even; consequently  $-C_0 = C_0$ . Hence  $-D = D$ . It follows that  $\text{Cay}(\mathbb{F}_q, D)$  is undirected. Now  $0 \notin D$ , we see that  $\text{Cay}(\mathbb{F}_q, D)$  has no loops. From definition, we deduce that  $\text{Cay}(\mathbb{F}_q, D)$  is a regular graph of valency  $|D|$ .

The restricted eigenvalues of  $\text{Cay}(\mathbb{F}_q, D)$ , as explained in [4, p. 136], are given by

$$\psi(\gamma^a D) = \sum_{x \in D} \psi(\gamma^a x),$$

where  $0 \leq a \leq N - 1$ . By (3.4) and Lemma 3.1, we have

$$\begin{aligned} \psi(\gamma^a D) &= \sum_{i=0}^{p_1^{m-1}-1} \psi(\gamma^a C_i) = \sum_{i=0}^{p_1^{m-1}-1} \tau_{i+a} \\ &= \frac{1}{N} \sum_{\chi \in C_0^\perp} g(\bar{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}). \end{aligned} \quad (3.5)$$

If  $\chi \in C_0^\perp$  and  $\chi = \chi_0$  (the trivial character), then  $g(\bar{\chi}) = -1$  and  $\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = p_1^{m-1}$ . If  $\chi \in C_0^\perp$  and  $\text{ord}(\chi) \neq 1$ , then  $\text{ord}(\chi) = p_1^\ell$ ,  $1 \leq \ell \leq m$  since  $\text{ord}(\chi) \mid |C_0^\perp|$ . For those characters  $\chi$  with  $1 \neq \text{ord}(\chi) < p_1^m$ , we have

$$\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = \chi(\gamma^a) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma)^i = \chi(\gamma^a) \frac{\chi(\gamma)^{p_1^{m-1}} - 1}{\chi(\gamma) - 1} = 0.$$

Thus, in (3.5), the terms corresponding to characters of order  $p_1^\ell$ ,  $1 \leq \ell \leq m-1$ , vanish. Hence (3.5) can be simplified to

$$\psi(\gamma^a D) = \frac{1}{N} [-p_1^{m-1} + \sum_{\chi \in C_0^\perp, \text{ord}(\chi)=p_1^m} g(\bar{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i})]. \quad (3.6)$$

Define a multiplicative character  $\theta$  of  $\mathbb{F}_q$  by setting  $\theta(\gamma) = \xi_N$ . Then  $\langle \theta \rangle = C_0^\perp$  since  $C_0^\perp$  is the unique subgroup of  $\widehat{\mathbb{F}_q^*}$  of order  $N$ . Thus any multiplicative character  $\chi$  of order  $p_1^m$  can be expressed as  $\theta^d$  for some  $d$  in  $(\mathbb{Z}/N\mathbb{Z})^*$ . We have

$$\psi(\gamma^a D) = \frac{1}{N} [-p_1^{m-1} + \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^*} g(\bar{\theta}^d) \sum_{i=0}^{p_1^{m-1}-1} \theta^d(\gamma^{a+i})] \quad (3.7)$$

For convenience, we set

$$S_a := \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^*} g(\bar{\theta}^d) \sum_{i=0}^{p_1^{m-1}-1} \theta^d(\gamma^{a+i}). \quad (3.8)$$

Let  $r$  be the positive integer given in Lemma 2.3 such that  $p^{-r}g(\bar{\theta}) \in O_K$ . By Lemma 2.2, we have

$$g(\bar{\theta}) = p^r(N_0\eta_0 + \cdots + N_{w-1}\eta_{w-1}), \quad (3.9)$$

where  $N_0, \dots, N_{w-1}$  are integers and  $\eta_0, \dots, \eta_{w-1}$  are defined in (2.1). From Lemma 2.1, we have  $g(\bar{\theta}^d) = \sigma_{d,1}(g(\bar{\theta}))$ . To simplify notation, we simply write  $\sigma_d$  for  $\sigma_{d,1}$ . It follows that

$$\begin{aligned} g(\bar{\theta}^d) &= \sigma_d(g(\bar{\theta})) = \sigma_d(p^r(N_0\eta_0 + \cdots + N_{w-1}\eta_{w-1})) \\ &= p^r(N_0\eta_0^{\sigma_d} + \cdots + N_{w-1}\eta_{w-1}^{\sigma_d}). \end{aligned}$$

Now writing  $d \in (\mathbb{Z}/N\mathbb{Z})^*$  as  $d = d_1 + p_1 d_2$ , where  $d_1 \in (\mathbb{Z}/p_1\mathbb{Z})^*$  and  $d_2 \in \mathbb{Z}/p_1^{m-1}\mathbb{Z}$ , we have  $\eta_j^{\sigma_d} = \sigma_d(\sum_{c \in \tilde{C}_j} \xi_{p_1}^c) = \sum_{c \in \tilde{C}_j} \sigma_{d_1 + p_1^{m-1}d_2}(\xi_{p_1}^c) = \eta_j^{\sigma_{d_1}}$ . We have

$$\begin{aligned} g(\bar{\theta}^d) &= p^r(N_0\eta_0^{\sigma_d} + \cdots + N_w\eta_w^{\sigma_d}) \\ &= p^r(N_0\eta_0^{\sigma_{d_1}} + \cdots + N_w\eta_w^{\sigma_{d_1}}) \\ &= \sigma_{d_1}(p^r(N_0\eta_0 + \cdots + N_w\eta_w)) \\ &= \sigma_{d_1}(g(\bar{\theta})) = g(\bar{\theta}^{d_1}). \end{aligned} \quad (3.10)$$

Hence (3.8) can be written as

$$\begin{aligned} S_a &= \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^*} g(\bar{\theta}^d) \sum_{i=0}^{p_1^{m-1}-1} \theta^d(\gamma^{a+i}) \\ &= \sum_{d_1 \in (\mathbb{Z}/p_1\mathbb{Z})^*} \sum_{d_2 \in \mathbb{Z}/p_1^{m-1}\mathbb{Z}} g(\bar{\theta}^{d_1 + p_1 d_2}) \sum_{i=0}^{p_1^{m-1}-1} \theta^{d_1 + p_1 d_2}(\gamma^{a+i}) \\ &= \sum_{d_1 \in (\mathbb{Z}/p_1\mathbb{Z})^*} \sum_{i=0}^{p_1^{m-1}-1} g(\bar{\theta}^{d_1}) \theta^{d_1}(\gamma^{a+i}) \sum_{d_2 \in \mathbb{Z}/p_1^{m-1}\mathbb{Z}} \theta^{p_1 d_2}(\gamma^{a+i}). \end{aligned}$$

Note that  $\sum_{d_2 \in \mathbb{Z}/p_1^{m-1}\mathbb{Z}} \theta^{d_2 p_1(a+i)}(\gamma) = 0$  if and only if  $p_1^{m-1} \nmid (a+i)$ . We only need to consider the terms for which  $p_1^{m-1} \mid (a+i)$ . For each  $0 \leq a \leq N-1$ , there exists a unique  $i_a \in \{0, 1, \dots, p_1^{m-1}-1\}$  such that  $p_1^{m-1} \mid (a+i_a)$ ; write  $a+i_a = p_1^{m-1}j_a$ ,  $j_a \in \mathbb{Z}/p_1\mathbb{Z}$ , we have

$$S_a = p_1^{m-1} \sum_{d_1 \in (\mathbb{Z}/p_1\mathbb{Z})^*} g(\bar{\theta}^{d_1}) \theta^{d_1}(\gamma^{p_1^{m-1}j_a}) = p_1^{m-1} \sum_{d_1 \in (\mathbb{Z}/p_1\mathbb{Z})^*} g(\bar{\theta}^{d_1}) \xi_{p_1}^{j_a d_1}. \quad (3.11)$$

For each  $j \in \mathbb{Z}/p_1\mathbb{Z}$ , define an additive character  $\psi_j$  on  $\mathbb{Z}/p_1\mathbb{Z}$  such that  $\psi_j(d_1) = \xi_{p_1}^{j d_1}$ . We have

$$\begin{aligned} S_a &= p_1^{m-1} \sum_{d_1 \in (\mathbb{Z}/p_1\mathbb{Z})^*} g(\bar{\theta}^{d_1}) \psi_{j_a}(d_1) \\ &= p_1^{m-1} p^r \sum_{i=0}^{w-1} \sum_{d_1 \in \tilde{C}_i} (N_0\eta_0^{\sigma_{d_1}} + \cdots + N_{w-1}\eta_{w-1}^{\sigma_{d_1}}) \psi_{j_a}(d_1) \\ &= p_1^{m-1} p^r [(N_0\eta_0 + N_1\eta_1 + \cdots + N_{w-1}\eta_{w-1}) \sum_{d_1 \in \tilde{C}_0} \psi_{j_a}(d_1) \\ &\quad + (N_0\eta_1 + N_1\eta_2 + \cdots + N_w\eta_0) \sum_{d_1 \in \tilde{C}_1} \psi_{j_a}(d_1) \\ &\quad \dots \\ &\quad + (N_0\eta_{w-1} + N_1\eta_0 + \cdots + N_{w-1}\eta_{w-2}) \sum_{d_1 \in \tilde{C}_{w-1}} \psi_{j_a}(d_1)]. \end{aligned} \quad (3.12)$$

Let  $M_0 = N_0 + N_1 + \cdots + N_{w-1}$ . Note that  $\sum_{i=0}^{w-1} \eta_i = -1$ . We continue the computations of  $S_a$  by considering two case.

**Case 1.**  $j_a = 0$ . In this case,  $\psi_{j_a}(d_1) = 1$  for all  $d_1 \in \mathbb{Z}/p_1\mathbb{Z}$ . It follows that  $\sum_{d_1 \in \widetilde{C}_z} \psi_{j_a}(d_1) = (p_1 - 1)/w$ ,  $0 \leq z \leq w - 1$ . Thus we have

$$S_a = \frac{p_1 - 1}{w} p_1^{m-1} p^r (N_0 \sum_{i=0}^{w-1} \eta_i + N_1 \sum_{i=0}^{w-1} \eta_i + \cdots + N_{w-1} \sum_{i=0}^{w-1} \eta_i) = \frac{1 - p_1}{w} p_1^{m-1} p^r M_0$$

**Case 2.**  $j_a \neq 0$ . In this case,  $j_a$  must belong to a unique coset of  $\langle p \rangle$  in  $(\mathbb{Z}/p_1\mathbb{Z})^*$ , say  $j_a \in g^t \langle p \rangle$ , where  $0 \leq t \leq w - 1$ . In this case, for any  $0 \leq z \leq w - 1$ , we have

$$\sum_{d_1 \in \widetilde{C}_z} \psi_{j_a}(d_1) = \eta_{\overline{z+t}},$$

where  $\overline{z+t}$  is the least nonnegative residue of  $z + t$  modulo  $w$ .

Define

$$\begin{aligned} K_0 &= \eta_0^2 + \cdots + \eta_{w-1}^2, \\ K_1 &= \eta_0 \eta_1 + \cdots + \eta_{w-1} \eta_0, \\ &\dots \\ K_{w-1} &= \eta_0 \eta_{w-1} + \cdots + \eta_{w-1} \eta_{w-2}. \end{aligned}$$

Then

$$\begin{aligned} S_a &= p_1^{m-1} p^r [(N_0 \eta_0 + N_1 \eta_1 + \cdots + N_{w-1} \eta_{w-1}) \eta_{\overline{t}} \\ &\quad + (N_0 \eta_1 + N_1 \eta_2 + \cdots + N_{w-1} \eta_0) \eta_{\overline{1+t}} \\ &\quad \dots \\ &\quad + (N_0 \eta_{w-1} + N_1 \eta_0 + \cdots + N_{w-1} \eta_{w-2}) \eta_{\overline{w-1+t}}] \\ &= p_1^{m-1} p^r [N_0 (\eta_0 \eta_{\overline{t}} + \eta_1 \eta_{\overline{1+t}} + \cdots + \eta_{w-1} \eta_{\overline{w-1+t}}) \\ &\quad + N_1 (\eta_0 \eta_{\overline{w-1+t}} + \eta_1 \eta_{\overline{t}} + \cdots + \eta_{w-1} \eta_{\overline{w-2+t}}) \\ &\quad \dots \\ &\quad + N_{w-1} (\eta_0 \eta_{\overline{1+t}} + \eta_1 \eta_{\overline{2+t}} + \cdots + \eta_{w-1} \eta_{\overline{t}})] \\ &= p_1^{m-1} p^r (N_0 K_{\overline{t}} + N_1 K_{\overline{t+1}} + \cdots + N_{w-1} K_{\overline{t+w-1}}) \end{aligned} \quad (3.13)$$

In Section 2, we have shown that  $w$  is even and  $f$  is odd. The Gauss periods  $\eta_j$  satisfy the following relations (see [18]):

$$K_{w/2} = (1 + (w - 1)p_1)/w, \quad K_j = (1 - p_1)/w, \quad \text{if } j \neq w/2.$$

Clearly there exists a unique element in the set  $\{\overline{t}, \overline{t+1}, \dots, \overline{t+w-1}\}$  that is equal to  $w/2$ , say  $\overline{t+h(a)} = w/2$ , where  $0 \leq h(a) \leq w - 1$ , and  $h(a)$  depends on  $a$ . We have

$$\begin{aligned} S_a &= p_1^{m-1} p^r \left[ \frac{1 - p_1}{w} (M_0 - N_{h(a)}) + \frac{1 + (w - 1)p_1}{w} N_{h(a)} \right] \\ &= p_1^{m-1} p^r \left( \frac{1 - p_1}{w} M_0 + p_1 N_{h(a)} \right). \end{aligned} \quad (3.14)$$

Therefore in this case, we have

$$S_a \in \{p_1^{m-1} p^r \left( \frac{1 - p_1}{w} M_0 + p_1 N_i \right) \mid 0 \leq i \leq w - 1\}.$$



Summing up, let

$$\begin{aligned} E = & \left\{ \frac{1}{p_1}(-1 + \frac{1-p_1}{w}p^r M_0) \right\} \\ & \cup \left\{ \frac{1}{p_1}(-1 + \frac{1-p_1}{w}p^r M_0) + p^r N_i \mid 0 \leq i \leq w-1 \right\}. \end{aligned} \quad (3.15)$$

We have shown that the restricted eigenvalues of  $\text{Cay}(\mathbb{F}_q, D)$  belong to  $E$ . Since  $|E| \leq w+1$ , we see that  $\text{Cay}(\mathbb{F}_q, D)$  has at most  $w+1$  distinct restricted eigenvalues. The proof of the theorem is now complete.  $\square$

Next we give necessary and sufficient conditions for  $\text{Cay}(\mathbb{F}_q, D)$  to be an srg. The proof uses discrete Fourier transforms, which were first employed in the proof of Theorem 3.1 in [19].

**Theorem 3.3.** *Let  $p_1$  be a prime,  $m \geq 1$ ,  $N = p_1^m$ . Let  $p \neq p_1$  be a prime,  $f = \text{ord}_N(p)$ ,  $w = \phi(N)/f$ , and  $q = p^f$ . Assume that  $-1 \notin \langle p \rangle$ ,  $\gcd(p(p-1), N) = 1$  and  $w \mid (p_1 - 1)$ . Let  $r$  be given in Lemma 2.3 and  $D$  be defined as in (3.4). Then  $\text{Cay}(\mathbb{F}_q, D)$  is a strongly regular graph if and only if there exists an integer  $\ell$ ,  $1 \leq \ell \leq w-1$ , such that*

$$\frac{p^r(1-p_1)\ell}{w} \equiv \epsilon \pmod{p_1} \quad (3.16)$$

and

$$p^s = \frac{\ell}{w} \left( p_1 - \frac{(p_1-1)\ell}{w} \right), \quad (3.17)$$

where  $s = f - 2r$  and  $\epsilon = \pm 1$ .

**Proof:** Suppose that  $\text{Cay}(\mathbb{F}_q, D)$  is a strongly regular graph. Then by Theorem 1.1,  $\text{Cay}(\mathbb{F}_q, D)$  has exactly two distinct restricted eigenvalues. By our computations of the restricted eigenvalues of  $\text{Cay}(\mathbb{F}_q, D)$  in the proof of Theorem 3.2, we must have  $N_i \in \{0, \epsilon\}$  for all  $0 \leq i \leq w-1$ , where  $\epsilon \neq 0$  is an integer. Thus (3.9) becomes

$$g(\bar{\theta}) = \epsilon p^r \sum_{i \in I} \eta_i,$$

where  $I = \{i \mid N_i = \epsilon, 0 \leq i \leq w-1\}$ . From  $|g(\bar{\theta})|^2 = p^f$ , we obtain that

$$\left| \sum_{i \in I} \eta_i \right|^2 = p^{f-2r} / \epsilon^2. \quad (3.18)$$

It follows that  $\epsilon$  must be a power of  $p$ . Since  $r$  is the largest power of  $p$  dividing the Gauss sum  $g(\bar{\theta})$  (see Lemma 2.3), we have  $\epsilon = \pm 1$ .

Let  $s = f - 2r$  and  $D' = \cup_{i \in I} \tilde{C}_i \subset (\mathbb{Z}/p_1\mathbb{Z})^*$ . From (3.18), we see that  $D'$  is a difference set in  $(\mathbb{Z}/p_1\mathbb{Z}, +)$  with parameters  $(p_1, \frac{p_1-1}{w}\ell, \frac{p_1-1}{w}\ell - p^s)$ , where  $\ell = |I|$ . From the basic parameter relation of difference sets, we obtain that

$$p^s = (\ell/w)(p_1 - (p_1-1)\ell/w).$$

Next we claim that  $\frac{p^r(1-p_1)\ell}{w} \equiv \epsilon \pmod{p_1}$ . This can be seen as follows.

$$\begin{aligned} \psi(\gamma^a D) &= \frac{1}{p_1^m}(-p_1^{m-1} + S_a) \\ &= \frac{1}{p_1}(-1 + \epsilon p^r(1-p_1)\ell/w) + p^r N_{h(a)}. \end{aligned}$$

Since  $\psi(\gamma^a D)$  are integers for all  $0 \leq a \leq N-1$ , we see that  $(1-p_1)\ell p^r/w \equiv \epsilon \pmod{p_1}$ .

Conversely, let

$$x = \frac{1}{p_1} \left( -1 + \frac{1-p_1}{w} p^r \ell \epsilon \right),$$

with  $\epsilon = \pm 1$ . By (3.16), we have  $x \in \mathbb{Z}$ . Define a function  $\varphi : (\mathbb{Z}/N\mathbb{Z}, +) \rightarrow \mathbb{Z}$  by

$$\varphi(a) := \frac{\psi(\gamma^a D) - x}{p^r}, \quad \forall a \in \mathbb{Z}/N\mathbb{Z}. \quad (3.19)$$

We note that since  $\psi(\gamma^a D)$  are algebraic integers, and by the computations in the proof of Theorem 3.2,  $\psi(\gamma^a D) = \frac{1}{p_1}(-1 + \frac{1-p_1}{w} p^r M_0)$  or  $\frac{1}{p_1}(-1 + \frac{1-p_1}{w} p^r M_0) + p^r N_{h(a)}$ , which are rationals, we must have  $\psi(\gamma^a D) \in \mathbb{Z}$ . It follows that  $\frac{1-p_1}{w} p^r M_0 \equiv 1 \pmod{p_1}$ . Now by assumption, we have  $\frac{(1-p_1)p^r \ell}{w} \equiv \epsilon \pmod{p_1}$ . Therefore

$$M_0 \equiv \epsilon \ell \pmod{p_1}.$$

We thus have  $\varphi(a) \in \mathbb{Z}$  indeed.

To simplify notation, we use  $G$  to denote the cyclic group  $(\mathbb{Z}/N\mathbb{Z}, +)$ . Then  $\widehat{G} = \{\nu^j \mid 0 \leq j \leq N-1\}$ , where  $\nu$  is the character of  $G$  sending 1 to  $\xi_N$ . The Fourier transform  $\hat{\varphi}$  of  $\varphi$  is given by

$$\hat{\varphi}(\nu^j) = \frac{\sum_{a \in G} \varphi(a) \nu^j(a)}{\sqrt{N}},$$

for  $0 \leq j \leq N-1$ .

When  $j = 0$ , we have

$$\hat{\varphi}(\nu^0) = \frac{\sum_{a \in G} (\psi(\gamma^a D) - x)}{\sqrt{N} p^r} = \frac{\sqrt{N}(-1 - p_1 x)}{p_1 p^r} = \sqrt{N} \frac{\epsilon(p_1 - 1)\ell}{w p_1} \quad (3.20)$$

For  $1 \leq j \leq N-1$ , we have

$$\begin{aligned} \hat{\varphi}(\nu^j) &= \frac{\sum_{a \in G} (\psi(\gamma^a D) - x) \nu^j(a)}{\sqrt{N} p^r} \\ &= \frac{\sum_{a \in G} \psi(\gamma^a D) \nu^j(a)}{\sqrt{N} p^r} \end{aligned} \quad (3.21)$$

By (3.7), we have

$$\begin{aligned} \hat{\varphi}(\nu^j) &= \frac{1}{p^r \sqrt{N}} \sum_{a \in G} \frac{1}{N} (-p_1^{m-1} + S_a) \nu^j(a) \\ &= \frac{1}{p^r N \sqrt{N}} \sum_{a \in G} S_a \nu^j(a) \\ &= \frac{1}{p^r N \sqrt{N}} \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^*} g(\bar{\theta}^d) \sum_{i=0}^{p_1^{m-1}-1} \theta(\gamma)^{di} \sum_{a \in G} \xi_N^{a(d+j)} \end{aligned} \quad (3.22)$$

If  $p_1 \mid j$ , then the (inner) sum  $\sum_{a \in G} \xi_N^{a(d+j)} = 0$  since  $d \in (\mathbb{Z}/N\mathbb{Z})^*$  (i.e.,  $d$  is relatively prime to  $N$ ); we thus have  $\hat{\varphi}(\nu^j) = 0$ .

If  $\gcd(p_1, j) = 1$ , then the (inner) sum  $\sum_{a \in G} \xi_N^{a(d+j)}$  is nonzero (and equals  $N$ ) if and only if  $j \equiv -d \pmod{N}$ ; in this case, we have

$$\hat{\varphi}(\nu^j) = \frac{1}{p^r \sqrt{N}} g(\theta^j) \left( \sum_{i=0}^{p_1^{m-1}-1} \xi_N^{-ji} \right).$$

Note that the above formula also holds true for those  $j$  such that  $1 \leq j \leq N-1$  and  $p_1 | j$  since  $\sum_{i=0}^{p_1^{m-1}-1} \xi_N^{-ji} = 0$  if  $p_1 | j$ . Therefore for all  $1 \leq j \leq N-1$ , we have

$$\hat{\varphi}(\nu^j) = \frac{1}{p^r \sqrt{N}} g(\theta^j) \left( \sum_{i=0}^{p_1^{m-1}-1} \xi_N^{-ji} \right). \quad (3.23)$$

Using the definition of  $\varphi$ , we have

$$\sum_{a \in G} \varphi(a) = \sum_{a \in G} \frac{\psi(\gamma^a D) - x}{p^r} = N \frac{-1 - xp_1}{p^r p_1} = \frac{N}{p_1} \cdot \frac{\epsilon(p_1 - 1)\ell}{w}. \quad (3.24)$$

From (3.20), (3.23) and Parseval's identity, we have

$$\begin{aligned} \sum_{a \in G} \varphi(a)^2 &= \sum_{j=0}^{N-1} |\hat{\varphi}(\nu^j)|^2 = |\hat{\varphi}(\nu^0)|^2 + \sum_{j=1}^{N-1} |\hat{\varphi}(\nu^j)|^2 \\ &= \frac{N(p_1 - 1)^2 \ell^2}{w^2 p_1^2} + \frac{p^s}{N} \sum_{j=1}^{N-1} \left| \sum_{i=0}^{p_1^{m-1}-1} \xi_N^{-ji} \right|^2 \\ &= \frac{N(p_1 - 1)^2 \ell^2}{w^2 p_1^2} + \frac{p^s}{N} \sum_{i,k=0}^{p_1^{m-1}-1} \left( \sum_{j=0}^{N-1} \xi_N^{j(k-i)} - 1 \right) \\ &= \frac{N}{p_1^2} \left( \frac{(p_1 - 1)^2 \ell^2}{w^2} + p^s (p_1 - 1) \right) \\ &= \frac{N}{p_1} \cdot \frac{(p_1 - 1)\ell}{w}, \end{aligned} \quad (3.25)$$

where in the last step of the above computations we used the condition (3.17). Let  $\kappa = \frac{N}{p_1} \cdot \frac{\ell(p_1 - 1)}{w}$  and  $S = \{a \in \mathbb{Z}/N\mathbb{Z} \mid \varphi(a) \neq 0\}$  (that is,  $S$  is the support of  $\varphi$ ). We have

$$0 \leq \sum_{a \in S} (\varphi(a) - \epsilon)^2 = |S| - \kappa.$$

On the other hand, from  $\sum_{a \in G} \varphi(a)^2 = \kappa$  and  $\varphi(a) \in \mathbb{Z}$ , we have  $\kappa \geq |S|$ . Therefore we must have  $|S| = \kappa$  and  $\sum_{a \in S} (\varphi(a) - \epsilon)^2 = 0$ . Hence  $\varphi(a) \in \{0, \epsilon\}$  for all  $a \in G$ . It follows that  $\psi(\gamma^a D)$ ,  $0 \leq a \leq N-1$ , take only two values. By Theorem 1.1,  $\text{Cay}(\mathbb{F}_q, D)$  is an srg. The proof is now complete.  $\square$

**Remark 3.4.** Condition (3.16) is equivalent to

$$\frac{p^b(1 - p_1)\ell}{w} \equiv \pm 1 \pmod{p_1} \quad (3.26)$$

This can be seen as follows. If we square both sides of (3.16), we obtain  $\frac{p^{2b+f-\tilde{f}}(1-p_1)^2\ell^2}{w^2} \equiv 1 \pmod{p_1}$ . Noting that  $p^f \equiv 1 \pmod{p_1}$  and  $p^{\tilde{f}} \equiv 1 \pmod{p_1}$ , we have  $\frac{p^{2b}(1-p_1)^2\ell^2}{w^2} \equiv 1 \pmod{p_1}$ . Since  $p_1$  is prime, we must have  $\frac{p^{b(1-p_1)\ell}}{w} \equiv \pm 1 \pmod{p_1}$ . The converse can be proved similarly. We comment that (3.26) is much easier to use since it does not involve  $m$  any more.

**Corollary 3.5.** *Let  $p_1$  be a prime,  $m \geq 1$ ,  $N = p_1^m$ . Let  $p \neq p_1$  be a prime,  $f = \text{ord}_N(p)$ ,  $w = \phi(N)/f$ , and  $q = p^f$ . Assume that  $-1 \notin \langle p \rangle$ ,  $\gcd(p(p-1), N) = 1$  and  $w \mid (p_1 - 1)$ . Let  $\tilde{f} = \text{ord}_{p_1}(p)$ ,  $D$  be defined as in (3.4), and  $\tilde{D}$  the subgroup of  $\mathbb{F}_{p^{\tilde{f}}}^*$  of index  $p_1$ . Then  $\text{Cay}(\mathbb{F}_q, D)$  is an srg if and only if  $\text{Cay}(\mathbb{F}_{p^{\tilde{f}}}, \tilde{D})$  is an srg.*

The proof is clear by Theorem 3.3 and the above remark. We omit the details.

#### 4. NEW INFINITE FAMILIES OF STRONGLY REGULAR CAYLEY GRAPHS

In this section, we give three infinite families of srg which are obtained by using Theorem 3.2 and Theorem 3.3.

**Example 4.1.** Let  $p = 11$ ,  $p_1 = 43$  and  $N = p_1^m$  for  $m \geq 1$ . It is easy to use induction to prove that  $\text{ord}_{43^m}(11) = \phi(43^m)/6$  for all  $m \geq 1$ . Let  $\mathbb{F}_q$  be the finite field of order  $q = 11^f$ , where  $f = \phi(43^m)/w$ ,  $w = 6$ . We claim that  $\text{Cay}(\mathbb{F}_q, D)$ , with  $D = \cup_{i=0}^{p_1^m-1} C_i$ , is an srg. We could use Corollary 3.5 together with the result in Table I to prove this claim. But we prefer to do it without relying on the result in Table I.

In this example, we have  $\tilde{f} = 7$  and  $b = 3$  (here  $b$  is obtained by computing  $\min\{b_0, b_1, \dots, b_5\}$  and  $b_j = \frac{1}{p_1} \sum_{z \in ([1, p_1-1] \cap \tilde{C}_j)} z$ ,  $0 \leq j \leq 5$ ). It follows that  $s = 1$ . Since  $\frac{3}{6}(43 - (43-1) \times \frac{3}{6}) = 11$ , (3.17) is satisfied with  $\ell = 3$ . Next  $\frac{3 \times (1-43) \times 11^3}{6} \equiv -1 \pmod{43}$ , we see that (3.26) is satisfied. It follows by Theorem 3.3 and Remark 3.4 that  $\text{Cay}(\mathbb{F}_q, D)$  is a strongly regular graph. This family of srg generalizes Example 5 in Table I.

**Example 4.2.** Let  $p = 5$ ,  $p_1 = 31$  and  $N = p_1^m$  for  $m \geq 1$ . It is easy to use induction to prove that  $\text{ord}_{31^m}(5) = \phi(31^m)/10$ . Let  $\mathbb{F}_q$  be the finite field of order  $q = 5^f$ , where  $f = \phi(31^m)/w$  with  $w = 10$ . Now  $\tilde{f} = 3$ . Let  $\tilde{D}$  be the subgroup of  $\mathbb{F}_{5^3}^*$  of index  $p_1 = 31$ . Then  $\tilde{D}$  is nothing but  $\mathbb{F}_5^*$ , i.e. the multiplicative group of the prime subfield of  $\mathbb{F}_{5^3}$ . Trivially  $\text{Cay}(\mathbb{F}_{p^{\tilde{f}}}, \tilde{D})$  is an srg. By Corollary 3.5,  $\text{Cay}(\mathbb{F}_q, D)$  with  $D = \cup_{i=0}^{p_1^m-1} C_i$  is an srg.

**Example 4.3.** Let  $p = 2$ ,  $p_1 = 127$  and  $N = p_1^m$  for  $m \geq 1$ . Again it is easy to use induction to prove that  $\text{ord}_{127^m}(2) = \phi(127^m)/18$ . Let  $\mathbb{F}_q$  be the finite field of order  $q = 2^f$ , where  $f = \phi(127^m)/w$  with  $w = 18$ . Now  $\tilde{f} = 7$ . Let  $\tilde{D}$  be the subgroup of  $\mathbb{F}_{2^7}^*$  of index  $p_1 = 127$ . Then  $\tilde{D}$  is nothing but  $\mathbb{F}_2^* = \{1\}$ . Trivially  $\text{Cay}(\mathbb{F}_{p^{\tilde{f}}}, \tilde{D})$  is an srg. By Corollary 3.5,  $\text{Cay}(\mathbb{F}_q, D)$  with  $D = \cup_{i=0}^{p_1^m-1} C_i$  is an srg. It should be noted that as an srg,  $\text{Cay}(\mathbb{F}_q, D)$  is not trivial at all.

## 5. CONCLUDING REMARKS

In conclusion, we generalize the construction in [11] to give new infinite families of srg. The main new result here is Theorem 3.3, which gives necessary and sufficient conditions for  $D$  in (3.4) to give rise to srg.

After finishing the research of this paper, we became aware of the very interesting paper [17] by Momihara. In [17], the author gave a recursive construction of strongly regular Cayley graphs, generalizing all 11 sporadic examples in the statement of the Schmidt-White conjecture into infinite families. In particular, the two index 6 examples are generalized into infinite families while we could only generalize one of the index 6 examples in this paper. However, the approach taken in our paper is different from that of [17] since ours is a direct construction. Also we obtained two conditions (3.16) and (3.17) which are necessary and sufficient for our construction to give rise to an srg. These conditions reveal an interesting connection between strongly regular Cayley graphs and cyclic difference sets in  $(\mathbb{Z}/p_1\mathbb{Z}, +)$ , which will be useful in future investigation of strongly regular Cayley graphs and cyclic difference sets.

## REFERENCES

- [1] Aubry, Y., Langevin, P., On the weight of binary irreducible cyclic codes, Workshop on Coding and Cryptography WCC'05 ( Springer ) **3969** Norway, 46–54 ( 2006 ).
- [2] Bose, R. C.: Strongly regular graphs, partial geometries, and partially balanced designs, Pacific J. Math. **13** (1963), 389-419.
- [3] Berndt, B. C., Evans, R. J., Williams, K. S.: *Gauss and Jacobi Sums*, A Wiley-Interscience Publication, New York, (1998).
- [4] Brouwer, A. E., Haemers, W. H.: *Spectra of Graphs*, Universitext, Springer-Verlag, New York, (2012).
- [5] Baumert, L.D., Mills, W. H., Ward, R. L.: Uniform Cyclotomy, Journal of Number Theory **14**, 67-82 (1982).
- [6] Calderbank, R., Kantor, W.M.: The geometry of two-weight codes, Bull. Lond. Math. Soc. **18** (2), 97-22 (1986).
- [7] De Lange, C.L.M.: Some new cyclotomic strongly regular graphs, J. Algebraic Combin. **4**, 329-330 (1995).
- [8] Feng, K., Yang, J., and Luo, S.: Gauss sum of index 4: (1) Cyclic case, Acta Math. Sin. (English Ser.) **21-6**, 1425-1434 (2005).
- [9] Feng, T., Xiang, Q.: Strongly regular graphs from unions of cyclotomic classes, J. Combin. Theory (B), in press, <http://dx.doi.org/10.1016/j.jctb.2011.10.006>.
- [10] Feng, T., Momihara, K., Xiang, Q., Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, available at [arXiv:1201.0701](https://arxiv.org/abs/1201.0701).
- [11] Ge, G., Xiang, Q. and Yuan, T.: Constructions of Strongly regular Cayley graphs using index 4 Gauss sums, J. Alg. Combin., in press, DOI 10.1007/s10801-012-0368-y.
- [12] Godsil, C., Royle, G.: Algebraic Graph Theory, Springer-Verlag, New York, Inc, (2001).
- [13] Ikuta, T., Munemasa, A.: Pseudocyclic association schemes and strongly regular graphs, European J. Combin. **31**, 1513-1519 (2010).
- [14] Ireland, K., Rosen, M.: A classical introduction to modern number theory 2nd Ed., Springer-Verlag, New York, (1990).
- [15] Langevin, P.: A new class of two-weight codes, in: S. Cohen, H. Niederreiter (Eds.), Finite Fields and Applications, Glasgow, 1995, in: London Math. Soc. Lecture Note Ser., vol. **233**, Cambridge University Press, 1996, pp. 181-187.
- [16] Ma, S. L., A survey of partial difference sets, Des. Codes Cryptogr. **4**, 221-261 (1994).
- [17] Momihara, K.: Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, available at [arXiv:1202.6414](https://arxiv.org/abs/1202.6414).
- [18] Thaine, F.: Properties that characterize Gaussian periods and cyclotomic numbers, Proc. AMS **124**, 35-45 (1996).

- [19] Schmidt, B., White, C.: All two-weight irreducible cyclic codes?, *Finite Fields and Their Appl.* **8**, 1-17 (2002).
- [20] Van Lint, J. H., Wilson, R.: *Combinatorics*, 2nd Ed, Cambridge Press, (2001).